(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号
特開2003－248578
（P2003－248578A）
(43)公開日　平成15年９月５日(2003.9.5)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　7/58		Ｇ０６Ｆ　7/58	Ａ	５Ｂ０３５
Ｇ０６Ｋ　19/10		Ｇ０９Ｃ　1/00	６５０Ｂ	５Ｊ１０４
Ｇ０９Ｃ　1/00	６５０	Ｇ０６Ｋ　19/00	Ｒ	

審査請求　未請求　請求項の数10　ＯＬ　外国語出願　（全 18 頁）

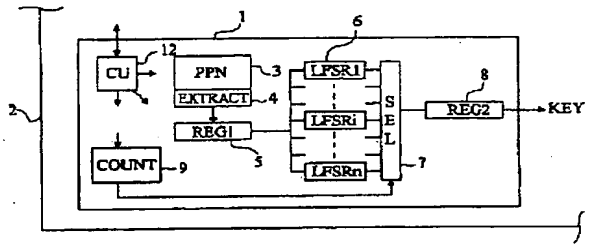
(21)出願番号　特願2002－347277(P2002－347277)
(22)出願日　平成14年11月29日(2002.11.29)
(31)優先権主張番号　０１１５５２９
(32)優先日　平成13年11月30日(2001.11.30)
(33)優先権主張国　フランス（ＦＲ）

(71)出願人　591035139
エステーミクロエレクトロニクス　ソシエテ　アノニム
フランス国，92120　モンルージュ，ブールバール　ロマン　ロラン，29番地
(72)発明者　リュク　ヴィダール
フランス国，　83910　プウリール，　ロティスマン　ル　カド，　12番地
(74)代理人　100074930
弁理士　山本　恵一

最終頁に続く

(54)【発明の名称】　集積回路識別の秘密量の発生

(57)【要約】
【課題】　集積回路の識別子に基づいて秘密量を発生させる方法と回路を提供する。
【解決手段】　最初のデジタルワードは、物理パラメータネットワークから発生され、前記最初のワードは、少なくとも１つのシフトレジスタに提供され、前記シフトレジスタの出力が、秘密量を発生させる。



1

【特許請求の範囲】

【請求項１】　集積回路（２）の識別子に基づいて秘密量（ＫＥＹ）を発生する方法において、
物理パラメータネットワーク（３）から最初のデジタルワードを発生させるステップと、
前記最初のワードを少なくとも１つの遡及シフトレジスタ（６）に提示するステップとを含み、前記シフトレジスタの出力が前記秘密量を形成することを特徴とする方法。

【請求項２】　前記最初のワードを複数の遡及シフトレジスタ（６）に提示し、それらシフトレジスタのうち１つを選択して前記秘密量（ＫＥＹ）を形成することを特徴とする請求項１に記載の方法。

【請求項３】　前記選択は、先行の秘密量の破棄の後に変更されることを特徴とする、請求項２に記載の方法。

【請求項４】　前記シフトレジスタ（６）は、線形遡及シフトレジスタであることを特徴とする請求項１に記載の方法。

【請求項５】　セレクタ（７）によって複数のシフトレジスタのうち１つを選択することを特徴とする請求項１に記載の方法。

【請求項６】　集積回路（２）の内部で秘密量（ＫＥＹ）を発生する回路において、
物理パラメータネットワーク（３）に基づく、集積回路チップに特定な最初のデジタルワードの発生器（４）と、
前記最初のワードを入力として受け取り、前記量を提供する少なくとも１つの遡及シフトレジスタ（６）と、
カウンタ（９）によってプログラム可能で前記シフトレジスタのドリフトシーケンスのセレクタとを含むことを特徴とする回路。

【請求項７】　集積回路（２）の内部で秘密量（ＫＥＹ）を発生する回路において、
物理パラメータネットワーク（３）に基づく、集積回路チップに特定な最初のデジタルワードの発生器と、
前記最初の２進ワードを入力として受け入れる遡及シフトレジスタ（６）と、
前記秘密量を提供する前記シフトレジスタのうちの１つを選択するセレクタ（７）とを含むことを特徴とする回路。

【請求項８】　前記セレクタにより行われた選択は、秘密データが破棄された場合に変更されることを特徴とする請求項６に記載の回路。

【請求項９】　セレクタ（７）は、前記シフトレジスタ（６）の入力／出力から、入力又は出力を選択するマルチプレクサにより形成されることを特徴とする請求項７に記載の回路。

【請求項１０】　請求項６に記載の回路において、
前記最初のワード及び前記秘密量を記憶するレジスタ（５、８）は一時レジスタであり、

2

前記回路は、予め決められた時間の後で、それら一時記憶素子をリセットする手段（１２）を含むことを特徴とする回路。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、集積回路からくるか又はそのような回路を含む電子サブアセンブリ素子からくる秘密量の使用に関する。例えば、本発明は、集積回路の識別又は認証のプロセスの秘密量として暗号鍵のようなプログラムによる、このような秘密量の使用に関する。より具体的には、本発明は、集積回路チップの製造に関連する、物理パラメータネットワークからくる集積回路のデジタル識別子の使用に関する。

【０００２】

【従来の技術】例えば集積回路チップを認証又はそれによって提供されるデータを符号化するための物理パラメータネットワークからくる識別子の使用は、集積回路中に隠された、又は埋め込まれた２進ワードを、不正コピーされる可能性のある記憶素子に一時的に記憶させずに使用することを可能にするため更に重要視されてきている。よって、起こり得る不正に対するシステムの信頼性は向上される。更に、物理パラメータネットワークの使用は所与の製造からくる異なる集積回路チップのための、互いに異なるデジタル識別子を得ることを可能にする。

【０００３】一般的には、集積回路のデジタル識別子は、遠隔システムに伝送するために可能な符号化又はスクランブルされた後、回路の外に提供される。後者（スクランブル）は、受信したワードを使用し、識別子を知ることを必要としない。

【０００４】本発明の応用例は、プリペイド又はプリペイドでない会計ユニット（count unit）からの金融取引に用いられるスマートカード分野に関するものであり、その通信にはスマートカードリーダと接触するものとしないものがある。

【０００５】もう１つの応用例は、ユーザ側に個人に特定されたデコーダを使用したデータ伝送システムである。そのような場合、デコーダは、そこに含まれる集積回路の物理パラメータネットワークからくる識別子を利用した認証回路を含んでもよい。支払システムにおけるスマートカードの例えで説明すると、認証がリーダとは異なるシステムによって行われる点は変えずに、リーダとそのスマートカードをユーザレベルで結びつけるのと同じことである。

【０００６】物理パラメータネットワークからくる識別子を使用することの不利益は、その個別で固定的な性質と関連する。

【０００７】よって、侵害者が識別子又はこの識別子を含むデジタルワード（認証量又は符号化鍵）に対する海賊行為に成功すると、集積回路を換える以外に解決方法

はない。実際、識別子に海賊行為がなされたことが疑われたら即その識別子の使用を中止することが安全な応用においては望ましい。この現象は一般的に符号化鍵もしくは認証又はより一般的に秘密量の破棄、として知られている。

【０００８】集積回路の物理パラメータネットワークの使用に基づいた鍵又は秘密量の破棄に対する解決策の欠如は、現在他の多くの用途に有利であるそれら識別子の使用を制限している。

【０００９】

【発明が解決しようとする課題】本発明の目的は、集積回路における物理パラメータネットワークからくるデジタル識別子の既知の問題点を克服することである。

【００１０】より具体的には、本発明の目的は、物理パラメータネットワークからくる識別子に基づいた秘密量又は鍵を、関わりのある集積回路を換えることなく破棄することを可能にすることである。

【００１１】破棄する場合は、物理パラメータネットワークの数を増やすことによって、使用可能なデジタル識別子の数を増やしてもよい。しかしそのような解決策は、集積回路が大きくなってしまうという問題点がある。しかも使用できる識別子の数は、依然としてとても少ない。

【００１２】更に、物理パラメータネットワークからくるワードのサイズより大きい秘密量のサイズは、検索されてしまう恐れがある。

【００１３】本発明のもう１つの目的は、物理パラメータネットワークによって集積回路識別子の個々の特性を排除することのない解決策を提供することである。

【００１４】また本発明は、集積回路の小型化と互換性のある解決策を提供することを目的とする。

【００１５】また本発明は、秘密量を更に安全なものにするために、秘密量利用システム側にとって透過的である、つまり後者（利用する側）が使用される手段を知る必要のない解決策を提供することを目的とする。

【００１６】

【課題を解決するための手段】これら及びその他の目的を達成するために、本発明は物理パラメータネットワークから最初のデジタルワードを発生させるステップと、前記最初のワードを少なくとも１つの遡及シフトレジスタに提示するステップとを含み、前記シフトレジスタの出力が前記秘密量を形成することを特徴とする、集積回路の識別子に基づく秘密量を発生する方法を提供する。

【００１７】本発明の実施形態によると、前記最初のワードは、複数の遡及シフトレジスタに提示され、それらレジスタのうち１つが秘密量を形成するために選択される。

【００１８】本発明の実施形態によると、前記選択は、先行の秘密量が破棄された後変更されるものとする。

【００１９】本発明の実施形態によると、前記１つ又は

複数のシフトレジスタは線形遡及シフトレジスタである。

【００２０】本発明の実施形態によると、シフトレジスタはセレクタによって複数ある中から選択される。

【００２１】本発明はまた、物理パラメータネットワークに基づく集積回路チップに特定な最初のデジタルワードの発生器と、前記最初のワードを入力として受け取り、前記量を提供する少なくとも１つの遡及シフトレジスタと、カウンタによってプログラム可能な前記シフトレジスタの導出シーケンス（derivation sequence）のセレクタとを含むことを特徴とする、集積回路の内部で秘密量を発生する回路を提供することを目的とする。

【００２２】本発明は更に、物理パラメータネットワークに基づく、集積回路チップに特定な最初のデジタルワードの発生器と、前記最初の２進ワードを入力として受け入れるものとする、いくつかの遡及シフトレジスタと、前記秘密量を提供する複数の前記遡及シフトレジスタのうち１つを選択するセレクタとを含むことを特徴とする、集積回路の内部で秘密量を発生する回路を提供することを目的とする。

【００２３】本発明の実施形態によると、前記セレクタによって行われる選択は、秘密データを破棄する場合に変更されるものとする。

【００２４】本発明の実施形態によると、セレクタは、シフトレジスタの入力／出力から入力又は出力を選択するマルチプレクサにより形成されている。

【００２５】本発明の実施形態によると、前記最初のワードと前記秘密量を記憶するレジスタは、一時的なレジスタであり、前記回路は、予め決められた時間の後でそれらの一時記憶素子をリセットする手段を含んでいる。

【００２６】本発明の前述した目的、特徴及び効果は、添付図面に関連して、以下に限定しない特定の実施形態の説明において詳述される。

【００２７】

【発明の実施の形態】明確にするために、集積回路の要素で本発明の理解に必要なもののみが図示され、以後説明される。具体的には、集積回路又は電子サブアセンブリ素子の構成部分であり本発明の物理パラメータネットワーク特性によって秘密量を発生することに関わらない部分については、示されていない。更に、本発明は、あらゆる従来の方法に応用することができるため、秘密量の利用（例えば認証又は符号化のプロセスによる）については、集積回路の内外に関わらず詳述していない。

【００２８】本発明の特徴は、少なくとも１つのシフトレジスタを、集積回路の製造に関連した最初のデジタルワードを提供する物理パラメータネットワーク、好ましくは線形遡及と結びつけることと、前記シフトレジスタによって提供されたデジタルワードを使用して集積回路の秘密量を形成することである。

【００２９】本発明によると、複数の線形遡及シフトレ

ジスタが機能的に使用されている。レジスタの数は、集積回路の発生の中で物理的に増やされてもよく、又は単一シフトレジスタが提供され、以後述べられるように異なるビットの導出が提供されてもよい。

【００３０】図１は、集積回路２の秘密量（ＫＥＹ）を発生するためのセル１の実施形態を簡潔にブロックで表している。

【００３１】セル１は、集積回路チップの製造に関わる物理パラメータネットワーク３（ＰＰＮ）を含む。物理パラメータネットワーク３は、多数の信号を提供し、また、前記物理パラメータネットワークを表して一時的に記憶要素５（ＲＥＧ１）に記憶され、２進ワードを抽出する回路４と連結している。

【００３２】例えば電気測定パラメータを含むあらゆるパラメータを使用することができる。それは例えばトランジスタのスレショルド電圧の測定、抵抗の測定又は浮遊容量の測定、電流源により発生された電流の測定、時定数（例えば、集積回路）の測定、振動周波数の測定等でもよい。それらの特性は、集積回路の技術的及び製造過程でのばらつきに影響されやすいため、考慮される電気パラメータはその製造に特定であり、その集積回路の署名を形成すると考えられる。

【００３３】電気パラメータ測定の例において、信号は、アナログーデジタル変換器によってデジタル信号に変換されてもよく、前記変換器は、抽出回路４を含み多重化されてレジスタ５に記憶される２進ワードを形成してもよい。

【００３４】時間測定を使用した回路も、物理パラメータネットワークとして使用されることができる。例えば、ＥＥＰＲＯＭ型メモリの読み出し／書き込み時間が測定される。この種類の物理パラメータネットワークの例は米国特許第５，８１８，７２８号において示されており、本発明の参考とした。

【００３５】本発明の参考とした仏国特許出願第０１０４５８５号において示されているような、フリップフロップに基づいた物理パラメータネットワークも更に使用することができる。

【００３６】本発明によると、鍵ＫＥＹは、物理パラメータネットワークから抽出した２進ワードを線形シフトレジスタに提示することにより得られる。

【００３７】図１に示される実施形態では、ｎ個の線形シフトレジスタ６（ＬＦＳＲ１、ＬＦＳＲｉ、・・・、ＬＦＳＲｎ）が提示されている。異なるレジスタのそれぞれの出力は、例えばセレクタ７（ＳＥＬ）に送られ、その出力が一時記憶素子８（ＲＥＧ２）において前記秘密量を提供する。あるいは、セレクタ７がレジスタ６の下流ではなく上流に配置されてもよい。

【００３８】使用される線形レジスタの選択、つまりセレクタ７の制御は、カウンタ９（ＣＯＵＮＴ）によって発生させられた２進パラメータ化ワードに基づいて行われ、よって前記カウンタは、現在の秘密量、即ち破棄されるまで使用される量を条件づける。セレクタはマルチプレクサでも、他の任意の従来の手段でもよい。

【００３９】前記カウンタは、前回使用されたデータの破棄後、秘密データが変えられる度に歩進される。カウンタ９はシフトレジスタのモジュロ数値ｎである。

【００４０】セル１は、集積回路１の安全な部分にあることが望ましい。「安全な部分」とは、直接電気測定による攻撃から保護されている部分である。例えばそれは、侵害者がその内容を検出しようとした場合溶解温度によってセルが破棄されるように、樹脂に埋め込まれたセルでもよい。

【００４１】図示されていないもう１つの実施形態によると、導出されたビットがパラメータ化される単一の線形シフトレジスタが使用される。この特徴は、以後図２及び図３との関連によって更に明らかになる。

【００４２】発生セル１は更に、それを形成する異なる要素を制御するためのセントラルユニット１２（ＣＵ）を含む。セントラルユニット１２は、秘密量の発生の制御信号を必要なときに、好ましくは一時的な方法で受けるため、また、破棄後の新しい秘密量の発生に必要な制御信号、つまりカウンタ９の増加（又は減少）を誘発する制御信号を受けるため、他の部分と共に集積回路の残りの部分と通信する。

【００４３】秘密量を使用するシステムは、秘密量ＫＥＹを処理するだけであってそれを発生させる方法を知る必要はない、という点が注目される。よって、本発明による発生セルは、秘密量の利用に対して透過的であり、よってあらゆる従来の利用法と互換性がある。

【００４４】他の方法としては、カウンタ９がセレクタ7を形成する多重化装置の選択コードのリストと置き換えられる。それらコードは使用に先立ってパラメータ化段階で不揮発性メモリに記憶される。

【００４５】線形シフトレジスタの使用は、秘密量の破棄を可能にすること、実現が容易であること、又より具体的に、先行の量を破棄する際集積回路の秘密量の変更を可能にする点で好ましく、一方、物理パラメータネットワークからくる識別子を利用し、そして特にそのような識別子は電気測定によって侵害できない、という利点を有する。

【００４６】図２は、遡及シフトレジスタの全体的な構成図である。このようなレジスタは、基本的にシフトレジスタ２０と遡及機能２１（ＲＥＴＲＯＡＣＴ）の２つの部分から成る。シフトレジスタ２０は任意のシフトレジスタ同様ビットＢ１、Ｂ２、Ｂ３、・・・、Ｂｍ－１、Ｂｍの連続を形成する。遡及機能を形成するブロック２１の機能は、ビットの連続のシフト毎に、レジスタに含まれるビットの少なくとも一部分の組み合わせに基づいて、シフトレジスタ（ビットＢｍ）の入力ビットを計算することである。よって、シフトレジスタ２０の各

ビットを遡及機能２１に個別に提供することができる。シフトレジスタ２０の出力は、直列形で該レジスタの２進ワードの最下位のビットＢ１によって形成される。並列出力の実施形態では、検索されたワードによって、前記シフトレジスタの全てのビットの値又はこれらビットの一部が同時にサンプリングされる。

【００４７】シフトレジスタの使用は、その実現がとりわけ容易である点で好ましい。遡及機能としては、任意の従来の機能が使用されることができる。出力として再生可能なワードを発生することが可能であるならば、非線形遡及機能の使用が考慮されてもよい。しかし、本発明の実施形態によると、前記シフトレジスタのいくつかのビットをＸＯＲ型に組み合わせた線形遡及機能が使用されている。これらビットのリストは一般的に「導出シーケンス（deriving sequence）」、又は「フィボナッチ構成（Fibonacci configuration）」という表現によって示されている。

【００４８】シフトレジスタに含まれる２進ワードの反復期間は、このレジスタのビット数だけではなく使用される遡及機能による。ｍビットの線形シフトレジスタにおいては、2^m-1の異なる２進シーケンスを使用できる。つまり、適応サイズのレジスタの出力ＯＵＴ上に提供される連続したビットをロードすることにより、2^m-1ビットまでの間のサイズの秘密量を得ることができる。これは、反復前で最も長いワードを形成する。線形シフトレジスタによって提供されたコードのアンローディングの連続を使用する事実は、物理パラメータネットワークによって提供されたワードの長さについて、秘密量を長くすることを可能にする。

【００４９】動作を分かりやすくするために、図３は導出シーケンスがＢ１、Ｂ４である４ビットの線形シフトレジスタを簡潔に表したものである。つまり、レジスタ２０´に含まれ、４ビットを超えるそれぞれ最下位のビットと最上位のビットであるＢ１及びＢ４は、遡及機能を形成するＸＯＲ型ゲート２１´によって結合される。ゲート２１´の出力はシフトレジスタ入力を形成し、よってＢ４入力となる。出力シーケンスＯＵＴは最下位ビット(Ｂ１)によって提供される。

【００５０】値を１０００として初期化すると仮定すると、つまり、他のビットを全て０にリセットした後Ｂ４に状態１をロードすると、レジスタ２０´の連続した内容はは反復前に１０００；１１００；１１１０；１１１１；０１１１；１０１１；０１０１；１０１０；１１０１；０１１０；００１１；１００１；０１００；００１０；０００１となる。

【００５１】本発明によれば、可能な組合わせの数による反復前の導出周波数の選択は、当業者であれば行うことができる。線形シフトレジスタの実現は、ハードウェア又はソフトウェアどちらの形であっても、全く従来どおりである。例えば、本発明の参考としたBruce Schneier著、Wileyにより出版された、第３９５～第４０１頁、「応用暗号法」第２版、を参照することができる。

【００５２】ネットワーク３からきて、レジスタ６の初期シーケンスの設定に使用されるワードは、直列又は並列でロードすることができる。レジスタ６の初期値を設定することにより、ユニット１２に制御されかつ好ましく予め決められた条件であるシフトレジスタの数は、再生可能な方法で得られた最終ワードを提供する。

【００５３】導出シーケンスを変更（図１のｎの連続のレジスタ６をもう１つ選択するのと同じことである）することによって、同一の入力ワード（ｍより大きい同じ数のシフトサイクルを持つ）のために得られた前記ワードが変更される。他の方法として、秘密量を変更するためにシフトサイクルの数が変更されてもよい。

【００５４】

【発明の効果】本発明の利点は、破棄防止方法（anti-revocation procedure）の要素をデータ利用システムに提供せずに、物理パラメータネットワークからくる２進ワードから得られた秘密量の破棄に関する問題を解決できる点である。よって、本発明により提供された解決策はとりわけ信頼性があり安全である。

【００５５】本発明の利点はいくつかの鍵の破棄を承認しながら１つの物理パラメータネットワークを使用できるという点である。

【００５６】本発明のもう１つの利点は、物理パラメータネットワークからくるワードの抽出に基づく秘密量の揮発性の（一時的）特性を保持できるという点である。

【００５７】もちろん、本発明は当業者であれば様々な改変、変更、改善等が容易に思いつくだろう。具体的には、使用される２進ワードの長さは応用によるものであり、本質的には集積回路に使用される認証プロセスによるものである。この点において、本発明は集積回路に提供された秘密量の既存の利用方法と互換性があると言える。

【００５８】更に、以上述べた機能的指示に従った遡及シフトレジスタの実施の実現は、線形であるか否かによらず当業者であれば行うことができる。シフトレジスタを複数使用するかレジスタを１つ使用するかの選択と、スイッチにより選択される導出シーケンスは例えば記憶素子とシフトレジスタの間で何が優先されるのが望ましいかによって行われることができる。

【００５９】更に、シフトサイクルの数は、所与の鍵に対して同じであれば重要ではない。破棄に伴う鍵の変更の際には他のサイクル数の設定も可能であり、それが同じ導出シーケンスを継続してもしなくてもよい。

【００６０】最後に、本発明はこれまでハードウェアの実現との関連をより詳しく説明してきたが、ソフトウェアの手段としても実現されることができる。

【００６１】このような変更、修正及び改良は、この開示の部分でしようとするものであり、本発明の思想及び

9

範囲の中で行われるものである。従って、前述した記載は、単に例としてであり、限定しようとするものではない。本発明は、特許請求の範囲及びその均等範囲によって規定するもののみに限定される。

【図面の簡単な説明】

【図１】本発明による秘密量を発生するための回路の実施形態をブロックで表した概要図である。

【図２】図１の回路で使用される線形遡及シフトレジスタのブロック図である。

【図３】第１及び第４ビットが導出された４ビットの線形遡及シフトレジスタの簡単な例である。

【符号の説明】

１　セル

10

２　集積回路

３　物理パラメータネットワーク

４　発生器、抽出回路

５　レジスタ、記憶素子

６　遡及シフトレジスタ、線形シフトレジスタ

７　セレクタ

８　レジスタ、一時記憶素子

９　カウンタ

１２　セントラルユニット

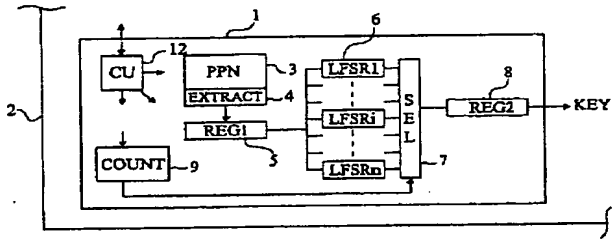
２０　シフトレジスタ

２０´　レジスタ

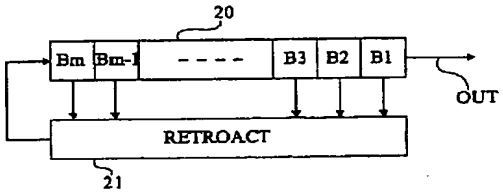
２１　遡及機能

２１´　ゲート

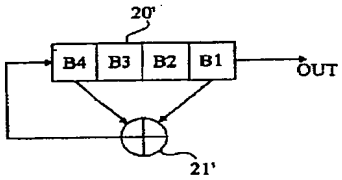
【図１】



【図２】



【図３】



フロントページの続き

(72)発明者　ミシェル　バルドゥイエ
フランス国，　13790　ルーセット，　カルティエ　フォンジュアーヌ

(72)発明者　ローラン　プラザ
フランス国，　13710　フェヴォー，　リュ　ドゥ　ジュー　デ　ブーレ，　レジダンス　レ　クロ

Ｆターム(参考)　5B035 AA13 BB09 CA11
5J104 AA16 AA18 EA08 FA04 NA04
NA22 NA23 NA25 NA26